STUDENT DATA AT RISK: A MULTI-TIERED APPROACH FOR MASSACHUSETTS TO MITIGATE PRIVACY RISKS WHILE UTILIZING INNOVATIVE EDUCATION TECHNOLOGY IN SCHOOLS

Kaleigh C. Fitzpatrick*

I. INTRODUCTION

Today, educators in Massachusetts, as well as across the country, have unprecedented access to innovative educational tools and technologies that enhance classroom teaching and learning. For instance, an elementary school teacher can discover, at no cost, an educational application ("app") based in the cloud[1] that could aid classroom instruction.[2] Aiming to assist students, the teacher quickly signs up for the app, sets up an account for each student, and incorporates the app within classroom instruction.[3] Although technological

* J.D. Candidate, Suffolk University Law School, 2016

[1] *See* Intellectual Property Group at Mintz Levin, *Saas, PaaS and the Cloud? Part 1: Hosted Services Basics for the Sourcing Professional – Software/Platform-as-a-Service*, NAT'L L. REV. (Apr. 8, 2014), *archived at* http://perma.cc/6M6R-E3EC (describing "the cloud" as shorthand for cloud computing which allows users to have access to software and numerous other technological resources in a centralized, remotely accessible location).

[2] *See* Steve Mutkoski, *Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel*, 30 J. INFO. TECH. & PRIVACY L. 511, 515 (2014) (depicting a typical set of circumstances under which education technology ("EdTech") apps are brought into the classroom).

[3] *See id.* (demonstrating the simplicity of using EdTech apps).

advances have enabled this seamless integration of education technology ("EdTech") into the classroom, the task of navigating the associated legal issues and tackling the privacy questions regarding students' data has proved to be a greater challenge.[4] Those issues are complex, and the questions remain largely unanswered.[5] By implementing the use of EdTech in classrooms, teachers and administrators are giving third-parties broad access to a range of information about students that is stored within the program, such as students' names, history of web activities, and responses to class assignments maintained in the app.[6]

Technological advances, which are driving reform within our classrooms nationwide, are expected to swell the amount of student data collected in the coming years.[7] In 2013, the pre-kindergarten through high school EdTech industry sales generated approximately $7.9 billion.[8] In today's data-driven society, every test score and every interaction with an online learning tool is now recorded.[9] The level of detail recorded in this data is alarming and can include a student's every diminutive interaction with an EdTech program.[10] Furthermore, these online tools can store and record students' feelings, amiability, and level of interest in the task, which can be analyzed and catalogued within complex data systems.[11] Thus, it is evident

[4] *See id.* at 519, 529 (discussing the risks and legal issues that arise through use of EdTech in schools).
[5] *See id.* at 528 (noting the unexpected associated concerns with use of the cloud in schools).
[6] *See id.* at 517 (explaining the largely unregulated access that EdTech third-party services have to student data through online programs).
[7] *See id.* at 511 (noting the rapidly increasing and broadening access to student data).
[8] *See* Natasha Singer, *With Tech Taking Over in Schools, Worries Rise*, N.Y. TIMES (Sept. 14, 2014), *archived at* http://perma.cc/YA5Y-DYJ2 (citing last year's massive sales in the education industry that demonstrate the universality of educational technologies in classrooms).
[9] *See id.* (indicating that present day school data collection is dramatically different than past practices).
[10] *See* Lisa Fleisher, *Big Data Enters the Classroom: Technological Advances and Privacy Concerns Clash*, WALL ST. J. (Mar. 23, 2014), *archived at* http://perma.cc/2F3C-KSXT (indicating the level of detail that EdTech apps can obtain from students).
[11] *See* Khaliah Barnes, *Student Data Collection is Out of Control*, N.Y. TIMES (Dec. 19, 2014), *archived at* http://perma.cc/VP94-P69F (demonstrating the capabilities

that student records now include infinitely more data points than historically collected by schools.[12] According to experts, however, when schools "'record and analyze students' every move and recorded thought, they chill expression and speech, stifling innovation and creativity."[13]

Legal concerns continue to mount as school districts struggle to quell the increasing pressure to implement available educational technology in classrooms and school administration.[14] The White House released a report on data and privacy in May 2014 stating that "[s]tudents and their families need robust protection against current and emerging harms, but they also deserve access to the learning advancements enabled by technology which promise to empower all students to reach their full potential."[15] Moreover, the U.S. Department of Education's Privacy Technical Assistance Center acknowledges that the Family Educational Rights and Privacy Act ("FERPA") does not always protect student information that is collected through online educational services.[16] FERPA exists as the primary federal law governing student privacy today.[17] Technologi-

of new data collection technologies and the type of information that can be captured).

[12] *See id.* (noting the significant changes in school administration due to technological advances).

[13] *See id.* (concluding that data collection technologies have the potential to stifle creativity and innovation because they are tracking students' every move).

[14] *See* JOEL REIDENBERG, et al., PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS 1 (2013) (suggesting that in order to keep pace with today's educational objectives, schools are implementing new technologies in their education and administration practices).

[15] *See* Jules Polonetsky & Omer Tene, *The Ethics of Student Privacy: Building Trust for Ed Tech*, 21 INT'L REV. OF INFO. ETHICS 25, 29 (July 2014) (noting the Obama Administration's focus on data and privacy).

[16] *Compare* Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232(g) (2015) (citing the existing federal authority protecting student data), *with* PRIVACY TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES, U.S. DEP'T OF EDUC. 2 (Feb. 2014) (noting that at present, FERPA regulations do not always protect student data maintained in the cloud).

[17] *See* FERPA, 20 U.S.C. § 1232(g) (2015) (providing the text of the main existing law governing student privacy).

cal developments in the educational arena have outpaced the protections under FERPA.[18] Therefore, it is time to confront and address the reality that our existing regulatory framework is currently ill-equipped to effectively regulate and protect students in this new age of EdTech.[19] After all, FERPA was enacted when schools stored student records in filing cabinets in the front office.[20]

Massachusetts is a recognized leader in the country for education;[21] now the intersection of technology and education presents its latest challenge for Massachusetts to maintain its distinguished record of educational excellence.[22] This Note will examine the current landscape surrounding student data privacy and provide recommendations specifically for Massachusetts to better protect students in this unprecedented era of technology. Section II provides a history of how and why cloud technology became so integrated in the school setting, along with an outline of the benefits and risks associated with that technology. In addition, this Section presents the current federal and state regulatory frameworks, specifically including an overview of the existing regulations in Massachusetts. Section III provides information on current developments across the country to strengthen and advance more comprehensive protections for student data with a particular focus on local efforts in Massachusetts. Section IV analyzes these efforts in Massachusetts, as compared to states across the country, within the context of overarching federal changes. Section V provides recommendations for Massachusetts to safeguard student data based on best practices and recent developments.

---

[18] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 3 (recognizing that FERPA is not always able to protect student data managed by third-parties in the cloud service). FERPA was enacted in 1974 and provides "certain minimum privacy protections for educational records." *Id. See also* REIDENBERG, *supra* note 14, at 3 (providing that FERPA has authority over educational agencies and institutions that receive federal funding).

[19] *See* Singer, *supra* note 8 (demonstrating the need for stronger privacy protections in schools).

[20] *See* REIDENBERG, *supra* note 14, at 3 (highlighting the changes in technology since FERPA was enacted in 1974).

[21] *See* Arne Duncan, *Under Deval Patrick, Mass. Has Led the Nation in Education*, BOS. GLOBE (Jan. 5, 2015), *archived at* http://perma.cc/76CY-STHP (noting Massachusetts's prominence in the nation's education system).

[22] *See* Eilen Rudden, *Will Technology be the Next Growth Sector?* BOS. GLOBE (Oct. 15, 2014), *archived at* http://perma.cc/7JJH-RSKY (addressing the convergence of education and technology).

II. HISTORY

A. Recent Changes in Technology and Schools' Use of Data

According to the U.S. Secretary of Education, Arne Duncan, "[student data] tells us where we are, where we need to go, and who is most at risk."[23] The U.S. Department of Education made it a "top national priority" to utilize student data as a mechanism to aid student performance and advance education.[24] School districts have always relied on student information to effectively manage schools and improve classroom learning; however, over the past few years, the development of new technologies now allows schools to more effectively pursue these goals.[25]

The student data landscape has recently shifted in three major ways: (1) private companies now often manage student data storage for schools in the cloud; (2) education technology has rapidly infiltrated classroom teaching and learning; and (3) a national movement to collect, store, and process student data has emerged.[26] Overall, there has been a rapid expansion of cloud technology not only in our daily lives, but also in elementary and secondary schools across the country.[27] In recent years, schools have incorporated the use of cloud

---

[23] *See* Arne Duncan, *U.S. Sec'y, Dep't of Educ., Fourth Annual Instution of Education Sciences Research Conference: Robust Data Gives Us the Roadmap to Reform*, U.S. DEP'T OF EDUC. (June 8, 2009), *archived at* http://perma.cc/2WQ2-4XKE (noting the importance of student data to make informed decisions for leaders in the education field).

[24] *See* Polonetsky & Tene, *supra* note 15, at 28 (noting the U.S. Department of Education's focus on student data).

[25] *See* DATA IN THE CLOUD: A LEGAL AND POLICY GUIDE FOR SCHOOL BOARDS ON DATA PRIVACY IN THE CLOUD COMPUTING ERA 3 (NAT'L SCH. BDS. ASS'N 2014) [hereinafter DATA IN THE CLOUD] (describing increased implementation of helpful technology in schools to protect students' private information); *see also* Polonetsky & Tene, *supra* note 15, at 27-28 (explaining the vast capability of new education technologies).

[26] *See* DATA IN THE CLOUD, *supra* note 25 (describing the recent changes within school districts related to cloud-based technology).

[27] *See* DATA IN THE CLOUD, *supra* note 25 (noting the undetected and pervasive presence of the cloud in today's society). Generally, "the cloud" refers to the "public cloud," which is a "large data center or centers that can span multiple geographic areas running the workloads of many customers at once, managed and owned by the provider" who maintains the data outside of the school's control. *Id.*

storage in its practices to store and interpret student data.[28] Before such technologies became available, K-12 public school districts in the United States would maintain their student and other data on hard drives managed internally by their own Information Technology departments.[29] Today, schools primarily utilize third-party cloud service providers, like Google Drive, that manage student data in the cloud and outside the physical bounds of the school.[30] As a result of these technological advances and subsequent shift in education practices, existing federal and state regulatory schemes have proven to be inadequate to protect students.[31] Under current laws, schools are unable to effectively protect student data from unintended third-party misuse when data is stored in the cloud by these outside companies.[32]

In the last decade, the education sector launched its national initiative to harvest the information reaped from big data called the Statewide Longitudinal Data Systems.[33] For the first time, "states and schools are capable of centralizing, organizing, searching, and

See also Polonetsky & Tene, *supra* note 15, at 27-28 (explaining the role of cloud service providers in school districts).

[28] *See* Fleisher, *supra* note 10 (explaining how schools are using cloud technology to collect and analyze data).

[29] *See* REIDENBERG, *supra* note 14, at 1 (describing how schools previously managed student data through in-house systems).

[30] *See* Jacob Kastrenakes, *Google Offers Schools Unlimited Drive Storage for Students and Teachers*, THE VERGE (Sept. 30, 2014), *archived at* http://perma.cc/YER8-FXEX (noting that cloud-based technologies, such as Google Drive, are now utilized by schools); *see also* Lon Berk, *After Jones, The Deluge: The Fourth Amendment's Treatment of Information, Big Data and The Cloud*, 14 J. HIGH TECH. L. 1, 8 (2014) (explaining that entities are now more commonly contracting with third-parties to manage their growing data needs instead of through their own systems).

[31] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 93-94 (2014) (noting that the law is not keeping pace with technology changes in schools).

[32] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 3 (pointing out that student data privacy law is being outpaced by the advances in technology).

[33] *See* Anya Kamenetz, *What Parents Need to Know About Big Data and Student Privacy*, NAT'L PUB. RADIO (Apr. 28, 2014), *archived at* http://perma.cc/873M-YU7Q (explaining the inception of the national Statewide Longitudinal Data System initiative). Big data are considered "extremely large datasets." *See id.* (defining big data in order to assist parents in their understanding of recent changes in student data privacy).

analyzing the information of millions of students, in ways that corporations have been doing for decades."[34] Many for-profit companies, such as Google, have joined this educational data push by providing software to gather and process student information.[35] This kind of vast amount of data, typically referred to as big data, can be analyzed to generate models capable of predicting further information about an individual or group based on data collected.[36] Today's classrooms are also increasingly employing data-driven EdTech to enhance teaching and learning.[37]

Cloud service providers offer data storage and management at lower costs, with greater flexibility, and the capacity to process, store, and analyze data for schools.[38] In the education context, "cloud-based platforms" come with many associated benefits.[39] For school administration, these tools are easy to use, can be accessed remotely at any time, and require limited staff maintenance.[40] For students, these tools provide an "individualized learning" experience while also preparing them specifically for standardized testing.[41] For teachers, these tools provide online forums through which teachers can

[34] *See id.* (describing the purpose of Statewide Longitudinal Data System to assist education stakeholders in making more productive decisions that are geared towards improvements in teaching and learning).
[35] *See id.* (noting the influential role that private companies have played in the Statewide Longitudinal Data System initiative).
[36] *See* Crawford & Schultz, *supra* note 31, at 98 (demonstrating that big data has the ability to predict personal information about an individual).
[37] *See* JULES POLONETSKY & JOSEPH JEROME, FUTURE OF PRIVACY FORUM, STUDENT DATA: TRUST, TRANSPARENCY AND THE ROLE OF CONSENT 1 (2014) (noting the need for technology in effective school administration and teaching in today's society); *see also Statewide Longitudinal Data Systems Grant Program: About the SLDS Grant Program*, U.S. DEP'T OF EDUC., *archived at* http://perma.cc/9QJS-MH6K [hereinafter *SLDS Grant Program*] (explaining that the rationale behind the State Longitudinal Data System is to allow education stakeholders to "make data-informed decisions to improve student learning and outcome").
[38] *See* REIDENBERG, *supra* note 14, at 1 (presenting the benefits of cloud technology in classrooms and schools).
[39] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (outlining the advantages of "cloud-based platforms" for schools).
[40] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (describing how these "cloud-based platforms" are easy to use and will increase school administration efficiency).
[41] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (highlighting the positive impact that cloud technology can have in schools).

share lesson plans.[42] The data collected through these tools on each student also provides teachers with in-depth information that assists in customizing individual learning plans with the hope of improved outcomes.[43] The social media component of these tools allows students to collaborate with peers in their own school or across many schools.[44] Schools' use of these online tools is quickly becoming the norm.[45] While these tools bring tremendous advantages, there are also serious attendant concerns that are often undetectable as student information is silently collected and misused.[46]

In 2005, in response to the No Child Left Behind mandate,[47] the Data Quality Campaign began developing a Statewide Longitudinal Data System intended for implementation in all 50 states.[48] If a

---

[42] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 1 (explaining how schools can benefit from utilizing online technology).

[43] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 1 (describing the ability to tailor teaching to the needs of individual students based on data collected through EdTech).

[44] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 1 (noting additional benefits of online educational services).

[45] *See* Johannes Britz & Michael Zimmer, *The Digital Future of Educ.: An Introduction*, 21 INT'L REV. OF INFO. ETHICS 2 (July 2014) (explaining that schools are increasingly utilizing these online tools in classroom instruction and school administration).

[46] *See id.* (describing the specific technology devices that can be used in the classroom).

[47] *See* Thomas Rentschler, *No Child Left Behind: Admirable Goals, Disastrous Outcomes*, 12 WIDENER L. REV. 637, 642 (2006) (providing the most recent iteration of the Elementary and Secondary Education Act of 1965 and the major federal law supporting elementary and secondary education); *see also* New America Foundation, *Federal Education Budget Overview*, FEBP NEW AMERICA, *archived at* http://perma.cc/9TKK-4CL5 (providing the background and rationale for the No Child Left Behind Act, including its strict requirements).

[48] *See* Steven Winnick, et al., *State Longitudinal Data Systems and Student Privacy Protections under the Family Educational Rights and Privacy Act*, PRIVACY & DATA SECURITY L. (2007), *archived at* http://perma.cc/9W42-5VYQ (describing the inception of the Statewide Longitudinal Data Systems ("SLDS")).

[49] *See id.* (presenting the reasons behind the creation of the Data Quality Campaign, which was a national collaborative effort). The Data Quality Campaign cites the following factors as requirements to participate in the Statewide Longitudinal Data System:

> (1) a unique statewide student identifier; (2) student-level enrollment, demographic, and program participation information; (3) the ability to match individual students' test records from year to year to measure academic growth; (4) information on untested

state implemented the Statewide Longitudinal Data System, it would receive a federal grant to support its efforts.[50] Then in 2009, the U.S. Department of Education declared that every state seeking federal funding under the Race to the Top[51] program must implement the Statewide Longitudinal Data System in order to receive that funding.[52] The Statewide Longitudinal Data System was created based on three main beliefs:

> (1) access to this data gives teachers the information they need to tailor instruction to help each student improve; (2) administrators can access the resources and information they need to effectively and efficiently manage; and (3) policymakers can rely on this data to evaluate which policy initiatives show the best evidence of increasing student achievement.[53]

> students; (5) a teacher identification system with the ability to match teachers to students; (6) student-level transcript information, including information on courses completed and grades earned; (7) student-level college readiness test scores; (8) student-level graduation and drop-out data; (9) the ability to match student records between the pre-K and postsecondary systems; (10) a state audit system assessing data quality, validity, and reliability.

Id. *See also* JOEL REIDENBERG & JAMELA DEBELAK, CHILDREN'S EDUC. RECORDS AND PRIVACY: A STUDY OF ELEMENTARY AND SECONDARY SCH. STATE REPORTING SYS. 21-22 (2009) (describing the origins of the Statewide Longitudinal Data System in school districts across the country).

[50] *See* Winnick, *supra* note 48, at 4 (explaining the federal government's use of awards as incentives for schools to participate in the SLDS program).

[51] *See* U.S. DEP'T. OF EDUC., RACE TO THE TOP EXECUTIVE SUMMARY 2 (U.S. DEP'T. OF EDUC.) (2009) (describing the Race to the Top program as a "competitive grant program designed to encourage and reward States that are creating the conditions for education innovation and reform; achieving significant improvement in student outcomes … and implementing ambitious . . . [education] plans").

[52] *See* Winnick, *supra* note 48, at 2 (describing further incentives for schools to participate in the grant program); *see also* U.S. DEP'T. OF EDUC., *supra* note 51, at 2 (describing the American Recovery and Reinvestment Act as "historic legislation designed to stimulate the economy, support job creation, and invest in critical sectors, including education" with $4.35 billion funding allocated to the Race to the Top program).

[53] *See* Winnick, *supra* note 48, at 9 (explaining the reasoning behind the inception of the Data Quality Campaign).

B. Regulatory Framework for Student Data

There are three federal statutes aimed at protecting this nation's youth from outside or online entities misusing their information.[54] First, FERPA[55] "governs the disclosure by school districts of student educational records."[56] Second, the Protection of Pupil Rights Amendment[57] regulates the disclosure of certain types of student information collected through surveys that intend to analyze the collected data.[58] Third, the Children's Online Privacy Protection Act[59] regulates the online collection of information from children.[60]

1. Family Educational Rights and Privacy Act

FERPA was enacted in 1974 and "provides certain minimum privacy protections for student educational records."[61] The statute governs any educational agencies and institutions that receive federal funding.[62] FERPA was "intended to protect the privacy of student

[54] *See* REIDENBERG, *supra* note 14, at 3 (outlining the three primary statutes that govern student data privacy).
[55] *See* Protection of Pupil Rights Amendment of 1978, 20 U.S.C. § 1232h (2015) (providing existing legislation working to protect student data).
[56] *See* REIDENBERG, *supra* note 14, at 3 (providing an overview of regulations under FERPA).
[57] *See* Protection of Pupil Rights Amendment of 1978, 20 U.S.C. § 1232h (2015) (ensuring that parents and students have protected rights when students are surveyed at school). The Protection of Pupil Rights Amendment seeks to ensure that parents have the opportunity to both review and opt out of any surveys that will be administered to their children. *Id.*
[58] *See* REIDENBERG, *supra* note 14, at 8 (describing the purview of the Protection of Pupil Rights Amendment).
[59] *See* Children's Online Privacy Protection Rule of 1998, 16 C.F.R § 312 (2015) (providing that any website directed at children or any websites through which the operator knowingly collects personal information from children under thirteen years old are required to give parental notice and obtain consent).
[60] *See* REIDENBERG, *supra* note 14, at 9 (outlining the protections available under the Children's Online Privacy Protection Act).
[61] *See* REIDENBERG, *supra* note 14, at 3 (noting that the most basic purpose of FERPA is to protect student records).
[62] *See* REIDENBERG, *supra* note 14, at 3 (outlining FERPA's limited jurisdiction governing only entities that receive federal funding).

educational records by regulating to whom and under what circumstances those records may be disclosed."[63] FERPA defines educational records as any information "directly related to a student" and "maintained by an educational agency or institution or by a party acting for such agency or institution."[64] The statute provides parents with the right to "inspect and review" the contents of their child's education records.[65] In addition, unless there is an applicable statutory exception for the disclosure, schools are prohibited from sharing student records or "personally identifiable information" without written parental consent.[66] Therefore, any student record maintained by the school is considered an educational record under FERPA and disclosure of that information to a third-party service provider must comply with FERPA requirements.[67]

There are several exceptions to FERPA's general mandate requiring parental consent for disclosure of educational records.[68] First, if all "personally identifiable information" has been removed

[63] *See* REIDENBERG, *supra* note 14, at 4-5 (explaining under which circumstances a student's record can be disclosed).
[64] *See* FERPA, 20 U.S.C. § 1232(g) (2015) (providing FERPA's definition of "educational records").
[65] *See* REIDENBERG, *supra* note 14, at 4 (noting a parent's right to amend incorrect information under FERPA).
[66] *See* Winnick, *supra* note 48, at 10 (highlighting the requirement of parental consent for disclosure under FERPA).
[67] *See* REIDENBERG, *supra* note 14, at 4 (explaining how FERPA applies to third-party providers). There are two types of educational records, "directory information" and "non-directory information." *Id.* Directory information can typically be disclosed without written consent from a parent and includes: "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most previous educational agency or institution attended by the student." *Id.* Disclosure of non-directory information requires prior written consent and includes "all other information related to a student and maintained by an educational agency or institution including, without limitation, social security numbers or student identification numbers." *Id.*
[68] *See* REIDENBERG, *supra* note 14, at 6 (discussing the exceptions to FERPA's parental consent requirement).

from the information being shared, then a student's record can be released without parental consent.[69] Second, consent is not required if student information is disclosed in connection with a research study conducted by the school, as long as the information is kept "confidentially and anonymously."[70] Third, "school officials with legitimate educational interests" can access students' educational records.[71] In 2008, this "school official" exception was expanded to third-parties, including contractors, consultants, or volunteers, as long as they operate under the "direct control" of schools.[72] Therefore, under this 2008 expansion, cloud service providers, such as Google and Microsoft, can now access student information.[73] In 2011, this exception was expanded further to allow schools to release information to "state officials" or an "authorized representative" during the "audit or evaluation" of programs.[74] The fourth exception permits a school or school district to disclose educational records to a third-party vendor for "research purposes," provided that the information remains confidential and the records are deleted after the agreed upon "research purpose" has concluded.[75]

Remedies for a FERPA violation are only available through administrative enforcement by the U.S. Department of Education and

[69] *See* REIDENBERG, *supra* note 14, at 6 (explaining that student records can be released without consent as long as any personally identifiable information has been removed).
[70] *See* REIDENBERG, *supra* note 14, at 6 (noting that data can be released for research study purposes as long as the research is performed "confidentially and anonymously").
[71] *See* REIDENBERG, *supra* note 14, at 6-7 (describing the FERPA exception for those entities with an "educational interest").
[72] *See* REIDENBERG, *supra* note 14, at 7 (presenting the recent amendment that allows access to student data for entities under "direct control" of the school and the seemingly unintended breadth of the "educational interest" exception).
[73] *See* REIDENBERG, *supra* note 14, at 7 (demonstrating the entrance of private companies in the student data arena).
[74] *See* REIDENBERG, *supra* note 14, at 7-8 (describing an additional expansion of the exceptions under FERPA).
[75] *See* REIDENBERG, *supra* note 14, at 7 (explaining the exception for projects with outside companies that ensure confidentiality and include a scheduled time to delete the data).

there are no enforceable legal penalties.[76] The U.S. Department investigates, processes, reviews, and adjudicates violations of FERPA.[77] Parents currently have no right to bring legal suit against a school for any alleged violations under FERPA.[78] In practice, the most potent enforcement mechanism for schools in violation of FERPA is to sanction the offending school by cutting off federal funding from the U.S. Department of Education.[79]

2. Massachusetts Student Data Infrastructure

The Massachusetts Department of Elementary and Secondary Education ("Department") is vested with the authority to request and receive student data from local schools and school districts to fulfill its administrative duties.[80] However, the Department's use of student data is regulated by the requirements of FERPA as well as the Massachusetts Fair Information Practices Act, G.L. c. 66A.[81] These laws require that personally identifiable student information is stored and maintained by the Department confidentially.[82] The school principal, "or his/her designee," is ultimately held responsible for "the privacy

[76] *See* Winnick, *supra* note 48, at 10 (citing Gonzaga University v. Doe, 536 U.S. 273 (2002) which held there is no right for parents, or others, to sue a school or educational agency for an alleged FERPA violation).
[77] *See* Winnick, *supra* note 48, at 11 (noting that the U.S. Department of Education is the entity with the authority to respond to FERPA violations).
[78] *See* Winnick, *supra* note 48, at 10 (explaining that under FERPA parents do not have standing to bring a legal suit against a school).
[79] *See* Winnick, *supra* note 48, at 11 (explaining that sanctions for violating FERPA include loss of federal funding); *see also* The New England Council, *Peering into Privacy*, NEW ENGLAND BD. OF HIGHER EDUC. (Feb. 17, 2015), *archived at* http://perma.cc/662D-MMLY (noting that the only sanction under FERPA is denial of federal education funds, which has never been used in practice).
[80] *See* MASS. DEP'T. OF ELEMENTARY AND SECONDARY EDUC., POLICIES RELATING TO THE COLLECTION AND USE OF STUDENT DATA 1 (2014) (noting that the Massachusetts Department of Elementary and Secondary Education ("Department") has the authority to obtain student data from individual schools).
[81] *See id.* at 3 (highlighting the limits on the Department's ability to collect student data); *see also* MASS. GEN. LAWS ch. 66A (2015) (providing the duties under the applicable Massachusetts law).
[82] *See* MASS. DEP'T. OF ELEMENTARY AND SECONDARY EDUC., *supra* note 80, at 1 (specifying that the Department is required "to keep personally identifiable data confidential").

and security of all student records maintained in the school."[83] The superintendent of schools is "responsible for the privacy and security of all student records that are not under the supervision of a school principal, for example, . . . student records of school-age children with special needs who have not been enrolled in a public school."[84] Schools will provide parents with their child's student records, if the parent requests this information.[85] Schools are also required to maintain a comprehensive log for each student record that denotes all persons who have accessed that record.[86] Furthermore, "no third-party shall have access to information in or from a student record without the specific, informed written consent" of the student or parent.[87] Requirements are stricter for "personally identifiable information" which is only released to third-parties "on the condition that he/she will not permit any other third party to have access to such information without the written consent" of the student or parent.[88] Schools are allowed to release "directory information," provided that public notice is given followed by a reasonable amount of time during which the parent or student can deny its release.[89] An appeals process, governed by the superintendent, is available to students or parents who feel a right has been violated.[90] If the parent or student

[83] *See* 603 MASS. CODE REGS. § 23.05 (2015) (providing the person(s) immediately responsible for student data in schools).
[84] *See id.* (describing the superintendent's overarching responsibility to protect student data privacy).
[85] *See* MASS. GEN. LAWS ch. 71, § 34H (2015) (detailing parents rights in relation to their child's student record).
[86] *See* 603 MASS. CODE REGS. § 23.07 (2015) (explaining the specific information that schools are required to collect on parties accessing any student record).
[87] *See id.* (requiring parental consent for a third-party to access student records).
[88] *See id.* (specifying that personally identifiable information, in particular, can only be released with parental consent).
[89] *See id.* (noting that student data that does not include personally identifiable information can only be released if the parent and/or student is given enough time and notice to decline such release). Directory information includes "a student's name, address, telephone listing, data and place of birth, major field of study, dates of attendance, weight and height of members of athletic teams, class, participation in officially recognized activities and sports, degrees, honors and awards, and post-high school plans." *Id.*
[90] *See id.* (outlining the opportunity for parents and students to appeal if they believe a privacy related right has been violated).

is not satisfied with the superintendent's decision on appeal, there is an option to bring a further appeal before the school committee.[91]

III. FACTS

A. Major Concerns Surrounding Student Data

Serious concerns are mounting that sensitive information, such as student learning disabilities or disciplinary history, is being collected and misused by third-party cloud service providers contracted by schools struggling to keep pace with rapidly evolving EdTech advancements.[92] Consequently, parents, students, and schools are losing control over private information and the limited protections under FERPA are insufficient to protect student data from service provider misuse.[93] One particularly alarming concern is that these third-party service providers have the capability to aggregate the student data and create profiles that could track each student throughout their elementary and secondary schooling.[94] The general fear is that these outside providers will then use the profiles for profit at the expense of students' privacy.[95] For instance, this data could be analyzed and used to inform and tailor commercial advertising that is then targeted back to those same students.[96] Moreover, because these "profiles" are tracking each student, the information collected could ultimately harm that student in some unpredictable way in the future.[97] Parental anxiety stems from the dread that these profiles could

[91] *See id.* (explaining the process for further appeal from the superintendent's decision).
[92] *See* Singer, *supra* note 8 (recognizing the complexities that arise with technological advances in education).
[93] *See* Singer, *supra* note 8 (noting the major concerns, most notably among parents, regarding the commercial use of student data).
[94] *See* Singer, *supra* note 8 (indicating parental concern that "personalized learning tools" are collecting information about students that could be used "to create a profile on a student, starting in elementary school" that could follow that child for life).
[95] *See* Singer, *supra* note 8 (explaining that third-party companies can profit from their misuse of student data).
[96] *See* Singer, *supra* note 8 (citing risks associated with commercial misuse of these technologies).
[97] *See* Singer, *supra* note 8 (specifying the concerns that parents have about the use of these educational technologies in the classroom).

be accessed by a future college admissions officer who will discount an applicant based on some minute data point captured in the student's past that should have no bearing on the present.[98]

A major concern with cloud service providers is that they often hold student data for an unregulated period of time, increasing chances for misuse.[99] Consequently, student data is susceptible to being misused for marketing purposes.[100] The following is an example demonstrating how cloud service providers can access student data for inappropriate marketing purposes, unless the school district's agreement with the provider specifically prohibits such use:

> A [school] district enters into an agreement [with a third-party service provider] to use an online tutoring and teaching program and discloses [students' personal information] from education records needed to establish accounts for individual students using FERPA's school official exception. The provider sends reports on student progress to teachers on a weekly basis, summarizing how each student is progressing. The provider collects metadata about student activity, including time spent online, desktop vs. mobile device, success rates, and keystroke information. If the provider de-identifies these metadata by

[98] *See* Singer, *supra* note 8 (explaining parents' concerns that improperly managed and unprotected student data could plague a child throughout life and hinder him or her in future pursuits).

[99] *See* REIDENBERG, *supra* note14, at 2 (presenting myriad concerns with these online technologies).

[100] *See* REIDENBERG, *supra* note 14, at 2 (discussing a particular concern that student data is used for marketing and advertising purposes by third-party providers); *see also* PRIVACY TECH. ASSISTANCE CTR., *supra* note 18, at 1 (describing how online education applications ("apps") collect student data). Online educational services oftentimes "collect a large amount of contextual or transactional data as part of their operations, often referred to as 'metadata.'" *Id.* Metadata is the "information that provides meaning and context to the other data being collected." *Id.* For instance, online tools can typically provide the amount of time a student needed to complete an assignment, but metadata can provide greater detail, including "the date and time when the student completed the activity, how many attempts the student made, and how long the student's mouse hovered over an item, which might indicate indecision." *See id.* at 2 (defining metadata and providing examples of the massive amount of information that can be collected on a student).

> removing all direct and indirect identifying information about the individual students (including school and most geographic information), the provider can then use this information to develop new personalized learning products and services . . . [legally under FERPA].[101]

School district information stored in the cloud is no longer under the school's "control" and is instead managed by third-parties on "shared servers."[102] Consequently, once student data is in the cloud, even if schools specifically draft the contract to maintain control over the data, sometimes this language is still inadequate to prevent third-party misuse.[103] When schools lose control over data through these agreements, risks abound and can include data breaches and intentional or unintentional exposure of data.[104] Additionally, two of the most undetectable yet dangerous risks occur when student data is gathered and analyzed by an outside company to inform targeted advertising or to sell to a third-party.[105]

Privacy concerns arise with EdTech because many of the services are marketed as "free" and instead generate revenue from mining and analyzing student data to develop individualized "marketing profiles" for each student.[106] These "ad-supported"[107] companies

---

[101] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 18, at 3 (highlighting how the third-parties are able to use student data for marketing purposes legally under FERPA).

[102] *See* DATA IN THE CLOUD, *supra* note 27, at 3 (explaining how cloud technology operates in the school context).

[103] *See* DATA IN THE CLOUD, *supra* note 27, at 3 (pointing out that school districts essentially lose control over student data when it is transferred to third-party providers).

[104] *See* DATA IN THE CLOUD, *supra* note 27, at 3 (describing the serious risks associated with student data misuse by private companies).

[105] *See* DATA IN THE CLOUD, *supra* note 25, at 3 (outlining the risks associated with the cloud).

[106] *See* Mutkoski, *supra* note 2, at 518 (explaining how third-party service providers can misuse student data for advertising purposes to generate a profit).

[107] *See* Cameron Evans, *Big Data's Opportunities, Responsibilities for Educ.*, INFO. WEEK (Feb. 21, 2013), *archived at* http://perma.cc/68LQ-DXLG (describing how "ad-supported" businesses operate). "Ad-supported" businesses are established with the "aim of gathering, examining, and making commercial use of the data that they hold for their customers." *Id.* These companies then process "user data" and generate "advertising and marketing profiles" for each of the users. *Id.*

have thrived in a broad spectrum of industries.[108] The education industry is prominently included on that list.[109] Moreover, despite the appeal of a "free" or "low-cost" service for schools, the harmful expense of privacy intrusions quickly outweigh any monetary savings.[110]

B. Current Efforts to Increase Protections for Student Data

1. Federal Efforts

In January 2015, President Obama proposed the Student Digital Privacy Act and in April 2015 the bill was introduced in Congress.[111] The Act is designed to "ensure that data collected in the education context is used only for educational purposes."[112] The Act is similar to the groundbreaking California statute and is intended to "prevent companies from selling student data to third-parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school."[113] The Act, however, would still support companies who use student

[108] *See* Mutkoski, *supra* note 2, at 518 (noting the success of ad-supported businesses in the private sector).
[109] *See* Mutkoski, *supra* note 2, at 518 (explaining how "ad-supported" businesses have had increasing success in the consumer services industry and teachers and schools have begun experimenting with new technologies in schools).
[110] *See* Mutkoski, *supra* note 2, at 518 (highlighting the major concerns associated with data mining).
[111] *See* H.R. 2092, 114th Cong. (2015) (presenting the text of the bill proposed in Congress that seeks to prohibit online services targeted at schools from using student data for advertising purposes); *see also* THE WHITE HOUSE, OFFICE OF THE PRESS SECRETARY, FACT SHEET: SAFEGUARDING AMERICAN CONSUMERS & FAMILIES (Jan. 12, 2015) (announcing a newly proposed student data protection entitled Student Digital Privacy Act); Corinne Lestch, *Obama Finds Bipartisan Backing for Student Data Privacy Pitch*, FEDSCOOP (Feb. 5, 2015), *archived at* http://perma.cc/3LXY-PC8Z (reporting on the bipartisan support for President Obama's proposed legislation to strengthen student data protections).
[112] *See* OFFICE OF THE PRESS SECRETARY, *supra* note 111 (describing the purpose of the Student Digital Privacy Act to prohibit commercial use of student data).
[113] *See* OFFICE OF THE PRESS SECRETARY, *supra* note 111 (noting the Student Digital Privacy Act's likeness to the recently enacted California legislation).

data to increase "student learning outcomes" through updates and enhancements to their educational services.[114] Additionally, in February 2015, "the House Education and the Workforce Subcommittee on Early Childhood, Elementary and Secondary Education [held] a hearing titled 'How Emerging Technology Affects Student Privacy.'"[115]

The U.S. Department of Education ("U.S. Department") founded the Privacy Technical Assistance Center ("Center") "as a one-stop resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to Statewide Longitudinal Data Systems and other uses of student data."[116] The Center is funded by a "government contract [and] provides technical assistance to education stakeholders through a range of materials and activities."[117] The Center is managed by the Chief Privacy Officer and works closely with the FERPA Working Group.[118] In February

[114] *See* OFFICE OF THE PRESS SECRETARY, *supra* note 111 (highlighting that the Act will not stifle updates to teaching and learning methods).
[115] *See* Amy Budner Smith, et al., *House to Move on Student Data Privacy*, NAT'L L. REV. (Feb. 11, 2015), *archived at* http://perma.cc/L75Q-EJVT (reporting on the House hearing on student data in February 2015); *see also* The New England Council, *Peering into Privacy*, NEW ENGLAND BD. OF HIGHER EDUC., *archived at* http://perma.cc/YN7L-V8DK (presenting the discussion topics covered in the House committee hearing, including possible amendments to FERPA and limitations on third-party companies' use of student data for advertising).
[116] *See* PRIVACY TECH. ASSISTANCE CTR., ABOUT PTAC, U.S. DEP'T OF EDUC. (2015) (explaining that the Privacy Technical Assistance Center ("Center") was established as a "comprehensive resource for education stakeholders to gain knowledge about privacy and security practices related to student data").
[117] *See id.* (describing the Privacy Technical Assistance Center's responsibilities to provide information, promote compliance with FERPA, and disseminate best practices for student data security). The Privacy Technical Assistance Center "provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems." *Id.*
[118] *See id.* (identifying the Chief Privacy Officer as highest authority overseeing the Center). The Center also works with the U.S. Department of Education's Privacy Advisory Committee, whose members include the Chief Statistician of National Center for Education Statistics, the Statewide Longitudinal Data System Program Officer, and representatives from the office of Federal Student Aid, the Office of Civil Rights, and the Office of Special Education and Rehabilitative Services. *Id.* The FERPA Working Group develops and scrutinizes new and existing privacy strategies and includes members from the Office of Management, the Family Policy Compliance Office, and the Office of General Counsel. *Id.*

2014, the Center disseminated guidance titled "Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices" to supplement gaps in federal laws protecting student data.[119] The U.S. Department recommends that schools go beyond the "minimum" required by these federal laws, and "adopt a comprehensive approach to protecting student privacy when using online educational services."[120] In January 2015, the Center announced "model terms of service" to assist schools in identifying which online educational services and apps have strong privacy and data security policies that will best protect students.[121]

The National School Boards Association ("Association") recommends that school districts "regularly review and update" policies related to student data privacy and security.[122] In order to better protect students, the Association also advises school districts to:

> (1) identify a district-wide Chief Privacy Officer or a group of individuals with district-wide responsibility for privacy; (2) conduct a district-wide privacy assessment and online services audit; and (3) establish a

[119] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 7-8 (recognizing the potential for privacy infringement because the existing federal laws do not protect against all improper uses of student data).

[120] *See* PRIVACY TECH. ASSISTANCE CTR., *supra* note 16, at 5 (elucidating the U.S. Department of Education's recommendation that schools must also individually make efforts to ensure the protection of their students' data).

[121] *See* PRIVACY TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: MODEL TERMS OF SERVICE, U.S. DEP'T OF EDUC. 1 (Jan. 2015) (providing "model terms of service" to aid schools in their use of available technology).

[122] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (highlighting the National School Boards Association's recommendation to school districts to review and rework existing policies to ensure protection of student data in light of the increasing use of technology in schools); *see also* Nat'l. Sch. Bds. Ass'n, *About Us*, NSBA.ORG, *archived at* http://perma.cc/VF8T-2FW3 (describing the mission of National School Board Association to influence key federal legislative issues). The National School Boards Association "represents state school boards associations and their more than 90,000 local school board members." *Id.* The Association "works with and through our State Associations … [and] advocates for equity and excellence in public education through school board governance." *Id.*

> safety committee or data governance team that includes the Chief Privacy Officer.[123]

The primary and critical objective for the safety committee or data governance team should be to facilitate an open dialogue with teachers, administrators, students, and parents, regarding the use of online educational services.[124] Furthermore, the team should act as the primary liaison between the school district and the school community on issues related to student data privacy.[125] The team should also carefully vet each educational app or tool before teachers or administrators utilize any outside technology services.[126] Additionally, the Association recommends that school districts develop a schedule to frequently assess and revise clear guidelines for school administrators seeking to implement online cloud services in their schools or school districts.[127] The team should also develop specific guidelines for how and when the district can contract with outside service providers.[128] If the district is allowed to contract under specified circumstances, the team should craft a standard written contract for such agreements.[129] This standardized contract should include terms that enable the district to maintain constant control over student data.[130] Further-

[123] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (encouraging school districts to create a group or position responsible for overseeing all student data privacy needs for the district).
[124] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (explaining a recommended role for safety committees to increase communication surrounding student data privacy issues).
[125] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (recommending that a student data governance team act as a "liaison between the school district and the community on privacy issues").
[126] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (providing comprehensive recommendations for schools to protect students data).
[127] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (suggesting that school districts should regularly update protocols regarding use of cloud service providers).
[128] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (discussing the importance of creating standardized contracts for agreements with private companies that include detailed protections for student data).
[129] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (specifying the conditions and restrictions that should be in place when schools contract with third-party vendors).
[130] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (highlighting the importance of detailed and specific contracts with third-party providers that include terms to ensure that school districts maintain "control" over student data).

more, school districts should have open and established lines of communication with students and parents through which comprehensible information is shared frequently to ensure that all parties are informed regarding their rights related to school data.[131] Finally, the Association recommends that school districts train staff to ensure that individual teachers are not making "unilateral decisions" to implement online services in the classroom without input from the safety committee or data governance team.[132]

In July 2014, Senator Edward Markey from Massachusetts and Senator Orrin Hatch from Utah introduced the "Protecting Student Privacy Act,"[133] aimed at establishing safeguards for student educational records.[134] The Act is intended protect student data in the hands of private companies through specific amendments to

[131] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (encouraging schools to have flexible terms that address and mitigate parents' and students' concerns).
[132] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (noting that teachers cannot be allowed to integrate new technologies into classrooms without following school protocols and ensuring that the technologies do not endanger student privacy).
[133] *See* Protecting Student Privacy Act of 2014, S. 2690, 113th Cong. (2014) (introducing this new legislation in the Senate on July 30, 2014); *see also* Protecting Student Privacy Act of 2015, S. 1322, 114th Cong. (2015) (reintroducing the bipartisan legislation in May 2015).
[134] *See* Protecting Student Privacy Act of 2014, S. 2690, 113th Cong. (2014) (providing the proposed federal legislation intended to amend FERPA to enhance student data protections); *see also* Press Release, *Markey, Hatch Introduce Legislation to Protect Student Privacy*, ED MARKEY UNITED SATES SENATOR FOR MASSACHUSETTS (July 30, 2014), *archived at* http://perma.cc/N5H4-W68Q (presenting the proposed legislation from Massachusetts and Utah senators to protect student educational records); Jake Williams, *Senate Bill Attempts to Modify FERPA in Era of Big Data*, FEDSCOOP (July 31, 2014), *archived at* http://perma.cc/H6MT-25LM (forecasting the potential impact that the proposed bill might have on student data privacy issues).

FERPA.[135] The Act requires that data security safeguards be implemented to protect sensitive student information maintained by private companies.[136] The Act encompasses six primary action items:

> (1) third-parties are required to destroy students' personally identifiable information when the information is no longer needed for the "specified purpose" for which it was shared; (2) the use of students' personally identifiable information to market a product is prohibited; (3) parents are provided with the right to access personal information about their children held by private companies and amend that information, which is the same right that they would have if the records were held by the school itself; (4) the name of all outside parties that have access to student information will be provided; (5) the amount of personally identifiable information that is transferred from schools to private companies will be minimized; and (6) private companies are not allowed to maintain detailed inventories on students in perpetuity.[137]

[135] *See* Protecting Student Privacy Act of 2014, § 2690, 113th Cong. (2014) (explaining that the bill is intended to amend FERPA to increase its protections in this new technology-driven society); *see also* Kristin Yochum, *Proposed Student Privacy Bill is Well-Intentioned but Unnecessary*, DATA QUALITY CAMPAIGN (July 31, 2014), *archived at* https://perma.cc/JTT2-VX28 (providing an alternative opinion regarding the impact the bill could have on the student data protection landscape).

[136] *See* Protecting Student Privacy Act of 2014, § 2690, 113th Cong. (2014) (providing that the overall purpose of the legislation is to protect student data maintained by private companies); *see also* Blake Neff, *Senators Seek to Improve Student Privacy*, THE DAILY CALLER (July 30, 2014), *archived at* http://perma.cc/WF2N-NLSY (noting the importance of restricting private companies' autonomy in their use of student data).

[137] *See* Press Release, *supra* note **Error! Bookmark not defined.** (focusing on amendments to FERPA that would protect student data when schools contract with third-party vendors); *see also* ISTE, *Student Data Privacy Bill Introduced, Int'l. Soc'y. for Tech. in Educ.*, CONNECTS BLOG (Aug. 5, 2014), *archived at* http://perma.cc/75Y8-DFDK (explaining in great detail all the specifications of the Act).

A Student Privacy Bill of Rights is another recently proposed mechanism to better protect students and their data.[138] The Director of the Student Privacy Project and administrative law counsel for the non-profit Electronic Privacy Information Center, Khaliah Barnes, is the main advocate behind the Student Privacy Bill of Rights.[139] The Bill of Rights "gives back to students control over information about their lives."[140] This Bill of Rights would be a "framework of enforceable rights" that is analogous to President Obama's Consumer Privacy Bill of Rights, which was announced in February 2012.[141] Khaliah Barnes argues that a Student Privacy Bill of Rights is necessary because under the existing regulatory infrastructure online service providers can gain control over student data legally under federal and state privacy laws and mine this data while schools and families are left powerless.[142] The proposed Bill of Rights includes six requirements.[143] First, "students have the right to access and amend" any kind of personal information that is "erroneous, misleading, or otherwise inappropriate," regardless of who has collected and is maintaining that information.[144] Second, "students have the right to reasonably limit [the amount of] student data [collected]" because companies should only be collecting data necessary to complete the

[138] *See* Valerie Strauss, *Why a Student Privacy Bill of Rights is Desperately Needed*, THE WASH. POST (Mar. 6, 2014), *archived at* http://perma.cc/NNX5-DLKE (discussing an additional proposal to protect student data in the form of a Student Privacy Bill of Rights).
[139] *See id.* (noting that the leading advocate behind the Student Privacy Bill of Rights is Khaliah Barnes).
[140] *See id.* (presenting an alternative protection strategy for student data); *see also* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECON. (2012) (providing an analogous framework for this type of bill of rights).
[141] *See* THE WHITE HOUSE, *supra* note 140 (relating the proposed Student Bill of Rights to President Obama's Consumer Privacy Bill of Rights).
[142] *See* THE WHITE HOUSE, *supra* note 140 (identifying the gaps that a Student Bill of Rights would fill in the current legislation).
[143] *See* Strauss, *supra* note 138 (noting the provisions included in the proposed Student Privacy Bill of Rights).
[144] *See* Strauss, *supra* note 138 (identifying strategies to provide students and parents with the right to ensure that personal data is accurate).

narrow purpose specified by the school or student.[145] Third, "students have the right to expect" that their data is never "repurpose[ed]" and is "collect[ed], us[ed], and disclos[ed]" only within the parameters in which the student provided that data.[146] Fourth, students should rightfully expect that schools and companies have safeguards in place to ensure "secure and responsible data practices."[147] Fifth, "students should have the right to clear, accessible," and transparent information regarding the kind of data collected, the ways the data will be used, and the attendant security protocols.[148] Sixth, "students should have the right to hold schools and private companies handling student data accountable" if these entities violate proper data security practices set forth in the Student Privacy Bill of Rights.[149]

2. Private Sector Efforts

Shortly after California enacted its revolutionary law, a number of major technology companies pledged to implement similar data privacy protections.[150] Since the President made reference to the Student Privacy Pledge ("the Pledge") as a baseline for his newly proposed Student Digital Privacy Act, the number of companies participating in the Pledge has rapidly increased to over two hundred.[151]

---

[145] *See* Strauss, *supra* note 138 (highlighting a second provision in the Student Privacy Bill of Rights that would allow students to limit the amount of personal data collected).

[146] *See* Strauss, *supra* note 138 (arguing that student data should only be used for its intended and agreed upon purpose).

[147] *See* Strauss, *supra* note 138 (emphasizing that students deserve to expect that their data will be protected by schools).

[148] *See* Strauss, *supra* note 138 (underlining the importance of transparency in the student data context).

[149] *See* Strauss, *supra* note 138 (suggesting that students should be able to hold schools and companies accountable for protecting their data).

[150] *See* Natasha Singer, *Microsoft and Other Firms Pledge to Protect Student Data*, N.Y. TIMES (Oct. 7, 2014), *archived at* http://perma.cc/TB4R-YNNH (reporting the reaction of private companies to the increase in action by state legislatures to better protect student data).

[151] *See id.* (noting the group of prominent companies that joined the Pledge to not misuse student data); *see also* STUDENT PRIVACY PLEDGE, *archived at* http://perma.cc/A3V8-LNAZ (providing the online version of the Student Privacy Pledge that includes over two hundred signatures as of January 2016).

The participating companies have made a firm public guarantee that they will never sell elementary and secondary student data.[152] Further, participating companies have pledged that, unless informed consent is received, they will not misuse student data in order to tailor advertisements or create individual profiles for students.[153] Section 5 of the Consumer Protection Act gives the Student Privacy Pledge legally enforceable authority.[154] The Federal Trade Commission ("FTC") can take legal action against companies that violate the terms of the Pledge, which is a public statement, and any actions contrary to that Pledge are considered public deception.[155] Precedent exists for legal enforcement of such promises as the FTC and attorneys general from several states have, in the past, taken legal action against companies who violated similar publicly made privacy promises.[156]

3. State Efforts

Over the course of 2013 and 2014, thirty-six states proposed over one hundred bills to regulate the collection and management of student data.[157] Ultimately, approximately thirty of these bills designed to strengthen student privacy protections were enacted into law.[158] Overall, the bills reiterated existing protections under FERPA, narrowly prohibited the collection of biometric data, and more broadly focused on general data management.[159] For instance,

---

[152] *See* Singer, *supra* note 150 (describing private companies' guarantee to refrain from using student data without consent).
[153] *See* Singer, *supra* note 150 (depicting companies' promise to act only with consent of involved parties).
[154] *See The Student Privacy Pledge and Security,* FUTURE OF PRIVACY FORUM, *archived at* http://perma.cc/HCW5-VS3S (stating that the Pledge is enforceable under the Federal Trade Commission ("FTC")).
[155] *See id.* (describing FTC's authority within the student data privacy context).
[156] *See id.* (noting that, in the past, action has been taken by the FTC in similar circumstances).
[157] *See* Singer, *supra* note 8 (citing the recent influx of legislation attempting to regulate the collection of student data).
[158] *See* Singer, *supra* note 8 (discussing the multitude of legislation introduced in the last year intended to increase protections for students and their data).
[159] *See* Singer, *supra* note 8 (summarizing the goals of the majority of recently proposed bills governing student data). A limited number of high school cafeterias

in Florida, school districts are now prohibited from "collecting unique biological data – called biometrics, including students' fingerprints or scans of the vein patterns in their palms."[160] Similarly, New Hampshire "prohibits students' email addresses, Social Security numbers, biometric data, criminal records, and information about family members from being stored in a state-run educational database."[161] In contrast, Colorado, Idaho, and West Virginia focus on transparency and require the publication of "lists of data points collected about students, such as race, ethnicity, disability status, disciplinary record, family financial status and medical conditions, like asthma."[162] Colorado school districts are now required to publish a list of the names of "third-party data warehouses, cloud services, learning apps and educational sites that are under contract with the education department and store student data."[163] North Carolina's board of education is now required to craft a strategic plan to protect student data and ensure compliance with FERPA.[164]

California's new legislation has been heralded as the most comprehensive student data privacy law to date.[165] In August 2014, California state legislators enacted a sweeping legislative reform "prohibiting educational sites, apps, and cloud services used by schools from selling or disclosing personal information about students" and from using students' data to tailor marketing efforts to those same students through "profile[s]" created from the collected

across the country now have the capability to utilize a "biometric identification system" that allows students "to pay for lunch by scanning the palms of their hands at the checkout line." *Id.*

[160] *See* Singer, *supra* note 8 (examining Florida's legislation focusing on biometrics).

[161] *See* Singer, *supra* note 8 (providing New Hampshire's decision to ban certain sensitive information from being stored in a state database).

[162] *See* Singer, *supra* note 8 (highlighting several states' efforts to ensure that any information collected on students is published).

[163] *See* Singer, *supra* note 8 (noting Colorado's emphasis on publicly publishing any information about third-party providers accessing student data).

[164] *See* Singer, *supra* note 8 (describing North Carolina's charge to the board of education and state officials to develop a plan to ensure data protection and compliance with FERPA).

[165] *See* Singer, *supra* note 8 (identifying California as leading the efforts to overhaul existing student data privacy protections).

data.[166] Student data under this law encompasses a broad range of information, such as "students' online searches, text messages, photos, voice recordings, biometric data, location information, food purchases, political or religious information, digital documents, or any kind of student identification code."[167] At present, California's law offers the most extensive and thorough set of reforms to date.[168] Senator Darrell Steinberg, the original sponsor of the legislation, states that this bill is "the first of its kind in the country to put the onus on Internet companies to do the right thing."[169] California's legislation is intended to "advance a fundamental principle of data rights for everyone: that a person who agrees to let a company collect personal details about them for a specific purpose has the right to decide whether that company may subsequently use that same information for unrelated activities."[170] To augment this reform, California legislators have also introduced another related student privacy bill regulating school contracts with education technology vendors.[171]

In summary, new state laws seeking to establish better data governance practices at the state and local levels are on the rise.[172] These laws have aimed to support in-depth investigations into student privacy issues and also require more "transparent and accessible"

[166] *See* Singer, *supra* note 8 (outlining the far-reaching stipulations included in California's new law).
[167] *See* Singer, *supra* note 8 (demonstrating the amount and array of data that the new California legislation protects from misuse by third-party vendors).
[168] *See* Singer, *supra* note 8 (noting that many other states have also enacted new student data privacy legislation while also emphasizing California's comprehensive coverage in comparison to other states).
[169] *See* Singer, *supra* note 8 (explaining that two of the main goals of the new legislation is to empower parents and students to have a voice in protecting their own personal information and to encourage private companies to join in the important data privacy efforts).
[170] Singer, *supra* note 8 (underscoring a basic principle that a person's data should not be used without that person's permission).
[171] *See* Singer, *supra* note 8 (presenting California's related bill that focuses on protecting student data specifically when schools contract with third-parties).
[172] *See* DATA QUALITY CAMPAIGN, STATE STUDENT DATA PRIVACY LEGISLATION: WHAT HAPPENED IN 2014, AND WHAT IS NEXT? (2014) (explaining that much of the newly proposed legislation focuses on governance issues).

data practices.[173] Many of the bills have also reinforced existing prohibitions.[174] Some states now also carefully control the "permissible activities of online service providers" through laws that have specific requirements for contracts between schools and providers.[175] These new requirements will also work to address parental concerns about data misuse.[176]

4. Massachusetts's Efforts

In August 2011, Massachusetts, as part of the Race to the Top initiative, began to develop a program with Collaborative Consulting that would meet federal regulations that require every state to systematically track and record student data for the Statewide Longitudinal Data Systems.[177] The new program, an online "teaching and learning platform," was completed and launched in November 2013.[178] The platform, called Edwin, presently reaches 80,000 educators in 2,000 Massachusetts public schools and includes data on one million active students and three million students in total.[179] Edwin allows the Massachusetts education system to store massive amounts of student information and enables that data to be fluidly shared within schools,

[173] *See id.* (highlighting the focus of the proposed legislation on transparency and research).
[174] *See id*. (noting that many of the proposed bills merely codified laws and practices that were already in existence).
[175] *See id*. (describing state laws that enforce specific regulations on private companies).
[176] *See id.* (emphasizing the important communications role that governance entities must play between schools, students, and parents).
[177] *See* SANDRA EDLER, COMMONWEALTH OF MASS. EXEC. OFFICE OF EDUC., A WINNING APPROACH TO EDUCATION 3 (2014) (explaining that the Edwin platform was intended to help Massachusetts adhere to federal regulations for tracking student data); *see also About Us*, COLLABORATIVE CONSULTING, *archived at* http://perma.cc/FTY4-SZPX (describing Collaborative Consulting as a company that works to "solv[e] business problems for clients"); U.S. Dep't of Educ., *supra* note 51 (describing Race to the Top as "a competitive grant program designed to encourage and reward states working towards education innovation and reform and achieving significant improvement in student outcomes").
[178] *See* EDLER, *supra* note 177, at 1 (noting the launch date of Edwin).
[179] *See* EDLER, *supra* note 177, at 2 (describing the widespread use of Edwin among Massachusetts school districts).

districts, and across the state.[180] Each student is assigned a unique identification number, which increases student privacy protection and anonymity.[181] With the emergence of Edwin, educators across the state now have access to detailed information about a student's journey through the entirety of the state's elementary and secondary education system.[182] The breadth and depth of information stored on Edwin, which is accessed by teachers and administrators in "near real-time" and through a "single online platform," is "unprecedented in Massachusetts—and perhaps the nation."[183]

In January 2013, Massachusetts introduced groundbreaking state legislation, Massachusetts Bill H. 331, which was the first bill of its kind to prohibit cloud service providers from "processing student data for commercial purposes."[184] On September 18, 2014, the House Committee on Education was authorized to conduct further investigation and study of the bill with regard to technology in educational institutions.[185] Then, as of January 6, 2015, the legislative records reflect that "no further action [has been] taken" on the bill.[186]

[180] *See* EDLER, *supra* note 177, at 2 (explaining Edwin's expansive storage capabilities); *see also* Benjamin Herold, *'Big Data' Research Effort Faces Student-Privacy Questions*, EDUCATION WEEK (Oct. 21, 2014), *archived at* http://perma.cc/5P6RJTMV (stating how schools store, share, and transfer student information).
[181] *See* EDLER, *supra* note 177, at 4 (highlighting Edwin's capabilities to protect student confidentiality).
[182] *See* EDLER, *supra* note 177, at 5 (providing teachers with access to student work almost immediately after submission).
[183] *See* EDLER, *supra* note 177, at 2 (commenting on the unprecedented data storage capabilities that Edwin brings to the Massachusetts education system).
[184] *See* H.331, 188th Gen. Ct., Reg. Sess. (Mass. 2013) (prohibiting service providers from processing student data for commercial purposes); Bradley Shear, *Mass. Bill to Ban Data Mining of Student Emails*, WIRED (Feb. 25, 2013), *archived at* http://perma.cc/VA86-7LN3 (noting that the proposed Massachusetts legislation is a trailblazer within the student data privacy context).
[185] *See* Order H.4463, 188th Gen. Ct., (Mass. 2014) (providing that on January 6, 2015, the current status reflects "no further action taken").
[186] *See* Order H.4463, 189th Gen. Ct. (Mass. 2015) (reflecting no further action).

IV. ANALYSIS

In order for Massachusetts to fully and effectively protect its students' data, stakeholders at the federal, state, and local levels must embrace a multi-tiered approach.[187] On the ground stakeholders, including parents, teachers, and administrators, must take an active and vigilant role in protecting student data and ensuring that laws, regulations, and procedures safeguarding students and their data are followed.[188] The Massachusetts legislature should enact the proposed Massachusetts Bill H. 331 in order to hold private companies accountable for potential misuse or abuse of student data.[189] In addition, schools and school districts in Massachusetts must continuously work towards developing the ground-level infrastructure necessary to ensure that student privacy is protected and that the new legislation is enforced.[190] The enactment of the Massachusetts law is vital to supplement the proposed federal legislation from Senators Markey and Hatch in order to comprehensively protect student data, because under FERPA and including the Markey-Hatch amendments, only student information encompassed within educational records is protected.[191] President Obama's Student Digital Privacy Act should be enacted because it also expands FERPA's limited scope of protection.[192] Although the proposed state and federal laws are both productive and necessary, additional measures are still needed and the Student Privacy Bill of Rights is the precise mechanism to fill the gaps in current laws and proposed frameworks.[193] Additionally, it

---

[187] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (presenting steps to increase protection for all student data stakeholders).
[188] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (recommending that parents and teachers remain cognizant of student data risks associated with new education technologies).
[189] *See* H.331, 188th Gen. Ct., Reg. Sess. (Mass. 2013) (providing that the purpose behind the proposed legislation is to prohibit commercial use of student data).
[190] *See* MASS. DEP'T. OF ELEMENTARY AND SECONDARY EDUC., *supra* note 80, at 3 (describing the organizational structure within the Department to manage student data).
[191] *See* Neff, *supra* note 136 (noting the limitations of FERPA and the Markey-Hatch Bill).
[192] *See* Lestch, *supra* note 111 (explaining that President Obama's proposed student data privacy legislation broadens the protections under FERPA).
[193] *See* Barnes, *supra* note 11 (highlighting the need for a Student Privacy Bill of Rights).

must be a joint effort between both the public and private sectors in order to protect students and their data.[194] Collectively, this multi-tiered approach at all levels—federal, state, local—and across both sectors—public and private—will effectively modernize the outdated laws and properly protect student data in the promising yet daunting age of metadata.

A. Massachusetts Schools and School Districts

Massachusetts is recognized as a leader in education and must be a pioneer in protecting student data in order to maintain this important tradition.[195] School districts in Massachusetts cannot allow teachers to implement outside educational apps into their classrooms without safety protocols and procedures.[196] Undoubtedly, the teacher's sole intention is to improve students' learning experiences with the educational app, but in reality, these tools can often take advantage of vulnerabilities in data security and silently misuse student data.[197] The Massachusetts Department of Elementary and Secondary Education's guidelines for contracting with third-party service providers should be utilized by schools when entering into any contract with outside technology companies.[198] These contracts do not,

[194] *See* Shear, *supra* note 184 (supporting a combined effort between the public and private sector to ensure data privacy protection).
[195] *See* Mutkoski, *supra* note 2, at 529 (recognizing Massachusetts as an advocate of protecting student data); *see also* Peter Balonon-Rosen, *Massachusetts Education Again Ranks No. 1 Nationally*, LEARNING LAB (Jan. 7, 2016), *archived at* http://perma.cc/Z48J-7AMV (affirming Massachusetts' national superiority in education).
[196] *See* Mutkoski, *supra* note 2, at 526-27 (indicating that school teachers and administrators must take care and proper precautions before introducing educational technologies into the classroom, which may put students' private data at risk).
[197] *See* Mutkoski, *supra* note 2, at 517-18 (contending that teachers are typically unaware of any associated student data privacy risks).
[198] *See* MASS. DEP'T. OF ELEMENTARY AND SECONDARY EDUC., *supra* note 80, at 3 (providing guidelines for schools that choose to contract with third-party service providers).

however, protect schools in their use of free, online, or "ad-supported" education apps.[199] Apps with hidden data mining and collection mechanisms are wrought with unregulated and inappropriate use of student data.[200]

Student data and its attendant privacy risks have prompted an awakening among teachers, parents, and students about the alarming risks that stem from the use of EdTech in classrooms.[201] Schools need to have strict protocols in place before educational apps are introduced into the classroom and teachers must understand the risks and diligently follow safety procedures.[202] Additionally, schools should have a dedicated person, such as a Chief Privacy Officer, who is trained in how to vet EdTech apps and more generally, protect the school or school district from data exploitation.[203]

Massachusetts should continue to invest in the development of the Edwin platform and expand its implementation across the state.[204] The Edwin platform is a mechanism through which Massachusetts can store all of its student educational data in one location, which satisfies schools' increasing data storage issues and eliminates the need for outside cloud storage services.[205] Furthermore, Edwin presents a solution to the current fragmented status of student data

[199] *See* Mutkoski, *supra* note 2, at 518 (demonstrating that even contracts are unable to protect student data when schools utilize certain types of educational technologies).
[200] *See* Mutkoski, *supra* note 2, at 518 (raising issues about the dangers of schools using free, online technologies).
[201] *See* DATA IN THE CLOUD, *supra* note 25, at 3 (providing recommendations for schools to better protect data); *see also* Singer, *supra* note 8 (noting the important role that each school has in protecting student data).
[202] *See* DATA IN THE CLOUD, *supra* note 25, at 4 (providing recommendations to protect student data when educational apps are implemented in the classroom); *see also* Singer, *supra* note 8 (presenting the major concerns associated with unregulated implementation of educational technologies in classrooms).
[203] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (recommending that schools create a Chief Privacy Officer position to oversee student data privacy issues).
[204] *See* EDLER, *supra* note 177, at 2 (reporting on the improvements that Edwin Analytics deliver to the Massachusetts education system).
[205] *See* EDLER, *supra* note 177, at 2 (connecting 80,000 educators across 400 school districts).

storage across Massachusetts and the country.[206] A unified data storage system gives teachers, administrators, and policymakers the ability to utilize data to help students in a more effective, efficient, and informed manner.[207] Garnering student data in a way that informs teaching is a powerful tool that could have an incredibly positive impact on the education system, and in turn, future generations in Massachusetts.[208] Finally, through Edwin, schools now have the capability to analyze and collect big data in ways that private companies have been doing for years.[209] With these new capabilities, schools can analyze data to expose trends and patterns for individual students or groups of students, more directly inform policy and decision-making, and more successfully educate students.[210]

The Edwin platform also offers broader educational benefits to students in Massachusetts.[211] In particular, the information sharing that Edwin facilitates between schools is a momentous achievement.[212] This progress is reflected in more streamlined efforts to close the education gap and universal access for all students to the highest quality teaching and learning materials.[213] A key component of Edwin's data analysis capabilities is early detection of students on

[206] *See* EDLER, *supra* note 177, at 2 (describing Edwin's capacity to store one million active students' information and approximately three million total students' information).
[207] *See* EDLER, *supra* note 177, at 2 (integrating communications between students, teachers, state agency analysts, policy-makers, superintendents, principals, and guidance counselors).
[208] *See* EDLER, *supra* note 177, at 2 (highlighting the fact that storing all student data on one platform is a major improvement within the Massachusetts education system which would be beneficial and an important investment for the future).
[209] *See* EDLER, *supra* note 177, at 5 (comparing the use of big data in the education context with corporate sector big data use).
[210] *See* EDLER, *supra* note 177, at 2 (noting that having all student data in one location will allow schools and educators to fully analyze the information in ways that will support improved learning and development initiatives).
[211] *See* EDLER, *supra* note 177, at 5 (presenting the broad range of potential benefits that Edwin brings to schools).
[212] *See* EDLER, *supra* note 177, at 5 (observing that one of the most influential benefits of Edwin is its capacity to share information among teachers across districts).
[213] *See* EDLER, *supra* note 177, at 6 (demonstrating the specific education improvements associated with Edwin, which allows better quality of education and learning for all students and teachers).

a path to dropping out.[214] With knowledge of this potential outcome early on, teachers and administrators can make adjustments immediately and work to prevent that possibility from becoming a reality.[215]

In light of this broader access, the need to preserve the anonymity of student data is even more critical.[216] Edwin provides each student with a "unique State Assigned Student ID" to protect anonymity.[217] However, it is not clear yet whether this type of protection is sufficient in the enigmatic era of big data.[218] Education officials claim that Edwin disseminates information in compliance with FERPA requirements.[219] However, loopholes or gaps in FERPA protections still leave student data vulnerable.[220] Therefore, despite these encouraging advancements in student data security, these efforts must persist and school administrators must continue to update privacy procedures according to unceasingly shifting dangers.[221]

The Edwin platform provides curriculum, teaching, and learning functions that can replace many of the services provided by outside EdTech companies, but unfortunately it does not have the capability to replace every service yet.[222] For example, Edwin is unable to replicate the services associated with clever and engaging online educational apps, leaving teachers and schools still looking to bring

---

[214] *See* EDLER, *supra* note 177, at 7 (highlighting a particularly promising benefit of the Edwin platform that will help to reduce dropout rates).
[215] *See* EDLER, *supra* note 177, at 7 (demonstrating how teachers can take advantage of Edwin's early detection capabilities to predict a student's likelihood to drop out of school).
[216] *See* EDLER, *supra* note 177, at 4 (noting Edwin's ability to freely and easily allow school districts to share information).
[217] *See* EDLER, *supra* note 177, at 4 (describing Edwin's safeguards to preserve student anonymity).
[218] *See* Herold, *supra* note 180 (highlighting the unknown future concerns surrounding mass collection of student data).
[219] *See* EDLER, *supra* note 177, at 1 (reporting that Edwin is fully compliant with the requirements under FERPA).
[220] *See* Privacy Technical Assistance Center, *supra* note 16, at 2 (noting that FERPA does not always protect student data in the cloud).
[221] *See* Herold, *supra* note 180 (demonstrating that data security requires constant revision and reevaluation of needs).
[222] *See* MASS. DEP'T OF ELEMENTARY AND SECONDARY EDUC., *supra* note 80, at 5 (demonstrating Edwin's capabilities to fulfill many school technology needs and fulfill any demand for risky EdTech).

EdTech apps into the classroom through outside companies.[223] Furthermore, concerns still remain regarding the massive amount of student data collected and stored in Edwin and the ways in which that data could follow students throughout life with harmful effects.[224] At this point, however, the long-term consequences of collecting vast quantities of sensitive data on students are largely unknown.[225] Even more concerning is that silent and almost undetectable data collection by outside companies could continue to appear harmless, but may have severely damaging consequences for those children as adults.[226]

In order to more consistently and completely protect student data, it is critical that school districts only consider contracting with companies committed to the Student Privacy Pledge to allow for some accountability in the event of data misuse.[227] The Pledge provides at least minimal remedies for school districts and holds companies publicly accountable for their promise to safeguard student privacy.[228] Presently, companies not participating in the Pledge are, for all intents and purposes, exempt from reproach, particularly because federal and state student privacy laws do not apply to most of the types of student data collected by online companies.[229] Furthermore, penalties under FERPA do not apply to private companies, only educational institutions whose federal funding can be pulled.[230] The Pledge, however, allows "the media, parents, educators, and federal

[223] *See* MASS. DEP'T OF ELEMENTARY AND SECONDARY EDUC., *supra* note 80, at 5 (describing Edwin's beneficial potential uses within school districts); *see also* EDLER, *supra* note 177 (noting the unprecedented technological capabilities that Edwin brings to school districts).
[224] *See* EDLER, *supra* note 177, at 6 (highlighting Edwin's capability to store vast amounts of student data for the use and benefit of the Massachusetts education system).
[225] *See* Singer, *supra* note 8 (identifying the unknown consequences of collecting massive amounts of data on children).
[226] *See* Singer, *supra* note 8 (indicating the potentially serious implications of collecting massive quantities of student data).
[227] *See The Student Privacy Pledge and Security*, *supra* note 154 (demonstrating the value of contracting with Pledge signatories).
[228] *See The Student Privacy Pledge and Security*, *supra* note 154 (explaining that the Pledge creates accountability for its signatories).
[229] *See* THE WHITE HOUSE, *supra* note 140 (explaining that gaps exist in the legislation that governs data collection by third-party companies).
[230] *See* Strauss, *supra* note 138 (noting the limited existing penalties for a FERPA violation).

regulators" to hold the signatories responsible for proper privacy and data security protections.[231] The success of the Pledge is, in large part, dependent on the resulting "public scrutiny" of companies who violate their promise to consumers.[232] Therefore, in order to foster a legitimate threat of public condemnation, all stakeholders must fully understand the Pledge's security requirements and remain vigilant for misuse.[233]

B. Massachusetts Student Privacy Law and Governance

The proposed Massachusetts legislation should be enacted because it shifts the onus of protecting student data from teachers and administrators onto private companies.[234] Our schools and teachers are already entrusted with the vital task of educating today's youth and student data protection should not fall solely to the teachers who already carry the weighty burden of educating our nation's future.[235] Through penalties, the Massachusetts Bill H. 331 would transfer this burden to private companies and require guarantees that student data will not be used for illegal commercial purposes.[236] This shift in responsibility is critical because it would lessen the intense pressure on parents, teachers, and school administrators to ensure the protection of student data at a time when risks associated technology use in

[231] *See The Student Privacy Pledge and Security*, *supra* note 154 (describing stakeholders' role in ensuring that companies uphold their commitment to the Pledge).
[232] *See The Student Privacy Pledge and Security*, *supra* note 154 (stating that the effectiveness of the Pledge relies on public scrutiny as an incentive for companies to abide by its terms).
[233] *See The Student Privacy Pledge and Security*, *supra* note 154 (noting the importance for stakeholders to understand the terms of the Pledge).
[234] *See* H. 331, 2013 Leg., 188th Sess. (Mass. 2013) (shifting the responsibility to protect student data from teachers and administrators to private companies); *see also* Shear, *supra* note 184 (reporting that the proposed legislation will hold private companies responsible for student data security).
[235] *See* Shear, *supra* note 184 (highlighting that the Massachusetts Bill H. 331 will shift responsibility of student data security to private companies).
[236] *See* Shear, *supra* note 184 (explaining that the proposed Massachusetts bill would be enforceable against private companies and would work to ensure that private companies do not misuse student data).

schools are complex and hastily escalating.[237] However, these stakeholders will still need to remain watchful, particularly because they will be the ground-level enforcers of this law.[238]

Schools and school districts must also bolster existing student data governance and security infrastructure.[239] In order to achieve that aim, school districts should adopt and implement the National School Board Association's recommendations, which include the identification of a district-wide Chief Privacy Office, or a group of individuals charged with overseeing student data protection.[240] In addition, school districts should assemble a "safety committee" or "data governance team," including the Chief Privacy Officer, responsible for evaluating online educational services before they are implemented in schools.[241]

Ultimately, it must be a shared effort between both the public and private sectors in order to most effectively protect student data.[242] The proposed Massachusetts law, if enacted, represents an important step forward in holding private companies accountable for misusing student data.[243] However, school districts also need to do their part to ensure on the ground enforcement and compliance with the mandates set forth in the legislation.[244] Schools and school districts should educate their teachers and administrators on privacy risks associated with online educational apps, which may be excellent tools for teach-

[237] *See* Shear, *supra* note 184 (noting that private companies would be required to take on a greater role in protecting student data).
[238] *See* Shear, *supra* note 184 (reiterating the continued need for stakeholders to monitor protections even if third-party companies are now being held accountable).
[239] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (noting the importance of establishing a group within school districts charged with overseeing student privacy issues).
[240] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (recommending that school districts create a Chief Privacy Officer position to manage student data privacy protections).
[241] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (suggesting that schools also form a committee dedicated to student privacy issues).
[242] *See* Shear, *supra* note 184 (supporting a combined effort between the public and private sectors to ensure data security).
[243] *See* Shear, *supra* note 184 (highlighting that the goal of the proposed Massachusetts legislation is to hold private companies accountable).
[244] *See* Shear, *supra* note 184 (suggesting that school districts should continue to play a major role in protecting student data).

ing and learning, but are often accompanied by serious risks for students.[245] This teacher-focused education will help to mitigate these risks, while also ensuring that these technologies are employed safely as innovative tools for improved education.[246]

If teachers want to utilize a new, cutting edge educational app in the classroom, it must first be vetted through the Chief Privacy Officer or a safety committee educated on how to spot red flags for privacy infringements that are harmful to students.[247] The Chief Privacy Officer or safety committee should implement the Department's recommendations for contracting with outside companies to thoroughly and consistently protect student data.[248] These strict contracting practices are necessary because even reputable companies like Google, if allowed, mine student data for advertising purposes.[249] For example, if graduated students use their school Gmail account through Google Apps for Education or link their personal YouTube or Google Plus accounts to their school Gmail, their data could be mined by Google or a third-party.[250] However, if the Massachusetts Bill H. 331 is enacted, it will stop private companies from being able to data mine student email accounts through enforceable legal sanctions.[251] Massachusetts is in dire need of a state law to ban data mining of students' class work and information, and this proposed law could be it.[252]

In order to increase transparency surrounding the use of student data, Massachusetts' school districts should publish a list of data

[245] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (outlining the multitude of risks associated with EdTech use in classrooms).
[246] *See* DATA IN THE CLOUD, *supra* note 25, at 2 (recommending specific education efforts to ensure that teachers understand student data privacy risks).
[247] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (suggesting that school districts have both a Chief Privacy Officer and privacy protection committee on staff).
[248] *See* DATA IN THE CLOUD, *supra* note 25, at 8 (providing recommendations for contracting with third-party service providers).
[249] *See* Shear, *supra* note 184 (reporting that even companies like Google are using student data for purposes unknown to students and parents).
[250] *See* Shear, *supra* note 184 (describing how Google could be misusing student data).
[251] *See* Shear, *supra* note 184 (noting the possible benefits of the newly proposed legislation in halting data mining).
[252] *See* Shear, *supra* note 184 (indicating that the proposed legislation could be effective in Massachusetts).

categories collected by the school on each student.[253] The recently enacted laws in Colorado, Idaho, and West Virginia require publication of this type of list so that parents and students know exactly what information is being captured and stored.[254] Transparency is critical because in order for students and parents to best protect themselves from privacy infringements, they need to know who has their data and exactly how it is being used.[255] Therefore, it is essential that schools meticulously track the precise items of student information being collected.[256] Massachusetts, like Colorado, should make public the list of outside companies that hold student data who are under contract with a school, school district, or Department of Education.[257] Documenting this type of information is crucial not only for transparency purposes, but also for better business practices so that schools know exactly which companies they are contracting with at all times.[258]

Interestingly, the model 2014 California legislation on student data privacy is remarkably similar to the 2013 law proposed in Massachusetts.[259] The California law, however, includes the additional provision that forbids educational tools and apps from using student data for commercial purposes.[260] Massachusetts should include such

[253] *See* Singer, *supra* note 8 (highlighting several states' focus on publishing a list of information collected on students to better inform students and parents about their data); *see also* Data Quality Campaign, *supra* note 172, at 5 (recommending that school work to increase transparency surrounding student data).
[254] *See* Singer, *supra* note 8 (highlighting several states' focus on transparency in the student data context); Data Quality Campaign, *supra* note 172, at 4 (summarizing efforts of several states to increase student data security).
[255] *See* Data Quality Campaign, *supra* note 172, at 5 (indicating that transparency is key in student data protection).
[256] *See* Data Quality Campaign, *supra* note 172, at 3 (noting that school record keeping and data tracking are crucial).
[257] *See* Singer, *supra* note 8 (explaining the importance of transparency and organized record keeping in relation to student data).
[258] *See* Singer, *supra* note 8 (highlighting several states' focus on increasing transparency between schools and parents); *see also* Data Quality Campaign, *supra* note 172, at 2 (indicating the critical nature of ensuring that schools document each and every third-party access to student data).
[259] *See* Singer, *supra* note 8 (describing the comprehensive newly enacted California legislation).
[260] *See* Singer, *supra* note 8 (reporting that California completely forbids companies, including those that provide educational classroom apps, from using student data for marketing purposes).

a provision because EdTech apps commonly use student data for commercial purposes and teachers unknowingly implement these apps in their classrooms leaving students unprotected.[261] Massachusetts should enact this bill because it will hold private companies accountable for misusing student data.[262] Furthermore, there is no downside to prohibiting online services from using student data for commercial purposes.[263] California is at the forefront of protecting student data and Massachusetts should be too.[264]

C. Federal Efforts Promise Greater Protections for Student Data

The Markey-Hatch bill, Protecting Student Privacy Act of 2014, should be enacted in addition to the Massachusetts Bill H. 331 because it will address several of the problematic gaps in FERPA.[265] Massachusetts Bill H. 331 is also necessary for Massachusetts to enact because the Markey-Hatch Act amends FERPA, which only applies to educational records, and the Massachusetts bill will ban commercial use of student data more broadly.[266] The Markey-Hatch bill will close the void under FERPA that allows companies to use student data for advertising purposes.[267] The federal bill will also give

[261] *See* Singer, *supra* note 8 (noting that use of educational apps in the classroom must be closely monitored).
[262] *See* Shear, *supra* note 184 (highlighting the promising benefits of the newly proposed legislation).
[263] *See* Singer, *supra* note 8 (suggesting that private companies should be banned from using student data for advertising objectives).
[264] *See* Singer, *supra* note 8 (recognizing California as a leader in the effort to protect student data).
[265] *See* Protecting Student Privacy Act of 2014, S. 2690, 113th Cong. (2014) (providing proposed amendments seeking to fill existing gaps in FERPA protections that have allowed misuse of student data); *see also* Protecting Student Privacy Act of 2015, S. 1322, 114th Cong. (2015) (reintroducing the proposed Act in May 2015).
[266] *See* Neff, *supra* note 136 (noting that certain types of data fall outside the purview of FERPA and the Markey-Hatch amendments).
[267] *See* Singer, *supra* note 8 (noting that many private companies are legally misusing student data); *see also* Strauss, *supra* note 138 (acknowledging that many federal and state privacy laws do not apply to data collected by online service providers).

parents and students the right to amend any incorrect personal information held by private companies.[268] This access for students and parents is critical because consequences for inaccurate information in the wrong hands could be serious and far-reaching.[269] The bill's focus on transparency is tremendously important, however, any concerns with transparency should be accomplished through state law and school district practices rather than through an amendment to FERPA.[270]

An additional concern is that even with the Markey-Hatch amendments, FERPA would still only protect student data that falls within the limited category of "education records."[271] Therefore, educational apps that capture data about student behavior or performance would still not be protected by FERPA.[272] This remaining gap in protection is particularly concerning in light of the increasing use of educational apps in the classroom capable of collecting a vast array of detailed information on students.[273] The type of data collected on students has drastically expanded since 1974 when FERPA was enacted.[274] Today, the majority of information collected by online services is not considered an educational record, and subsequently will be left unprotected under the Markey-Hatch bill.[275] Therefore, unless FERPA is amended to expand beyond protecting only "educational records," state laws and school districts need to step in and protect student data that fall outside of this extremely limited category.[276] This Massachusetts bill is most assuredly a step in the right

[268] *See* Strauss, *supra* note 138 (highlighting the importance of giving students access to amend incorrect personal information).
[269] *See* Strauss, *supra* note 138 (explaining that an individual has a due process right to ensure that his or her own personal information is accurate).
[270] *See* Williams, *supra* note 134 (arguing that aspects of the proposed legislation are not necessary in order to achieve the desired results).
[271] *See* Neff, *supra* note 136 (highlighting the limitations of FERPA). Education records include a student's personally identifiable information. *Id.*
[272] *See* Neff, *supra* note 136 (providing examples of which types of data fall outside the parameters of FERPA governance).
[273] *See* Neff, *supra* note 136 (indicating the gaps in protections under FERPA).
[274] *See* Neff, *supra* note 136 (explaining that FERPA only protects certain student data, leaving other data unprotected and subject to misuse).
[275] *See* Neff, *supra* note 136 (highlighting the gaps in protection under FERPA and the Markey-Hatch bill).
[276] *See* Neff, *supra* note 136 (noting that the protections under FERPA and the Markey-Hatch bill are limited).

direction to tackle the most immediate worries regarding student data, commercial misuse.[277] However, in order to comprehensively protect student data, a multi-tiered approach is required and dedicated efforts must be enlisted at all levels and from all stakeholders.[278]

President Obama's Student Digital Privacy Act offers additional protections for students and should be enacted along with the Markey-Hatch Bill.[279] The Student Digital Privacy Act defines student data more broadly than the limited Markey-Hatch definition and includes protections for "personally identifiable information."[280] The Act is based on the Student Data Privacy Pledge that has been signed by over two hundred private technology companies.[281] The Act would set a baseline threshold for student data privacy protection and leaves room for states to implement more stringent protections.[282]

The proposed Student Privacy Bill of Rights ("Bill of Rights") should be the privacy framework that stakeholders, including those in the private sector, implement to ensure that students maintain control over their own data.[283] The Bill of Rights will be legally enforceable when companies, subject to Federal Trade Commission jurisdiction, "publicly and affirmatively" adopt it.[284] The Bill of Rights gives students the authority to view collected information and correct inaccurate information, which is an important right that current laws and proposed frameworks do not provide

[277] *See* Neff, *supra* note 136 (reporting that the Markey-Hatch bill's primary purpose is to ban commercial use of student data).
[278] *See* Neff, *supra* note 136 (presenting the bill as a federal level change to better protect student data).
[279] *See* H.R. 2092, 114th Cong. (2015) (providing comprehensive protections for students and their data specific to commercial misuse of student data); *see also* Lestch, *supra* note 111 (discussing an additional federal level authority to improve student data security).
[280] *See* Neff, *supra* note 136 (describing how the Student Digital Privacy Act defines student data).
[281] *See* Lestch, *supra* note 111 (noting support from large, technology companies, such as Google, for the Student Privacy Pledge).
[282] *See* Lestch, *supra* note 111 (characterizing the bill as a starting point, giving states leeway to add additional protection).
[283] *See* Strauss, *supra* note 138 (describing the purpose for the proposed Bill of Rights).
[284] *See* THE WHITE HOUSE, *supra* note 140 (discussing the enforceability of the Bill of Rights).

for.[285] Additionally, EdTech companies should be limited to "collect[ing] only as much student data as they need to complete specified purposes" initially authorized by the school.[286] Issues arise because these "specified purposes" are often defined vaguely as "educational purposes" or "educational quality" and consequently allow companies to collect vast amounts of data under ambiguous, but permissible authority.[287] Instead, schools should be more specific and state, for example, that data collection is permissible when necessary to "improve fifth grade reading skills."[288] Furthermore, schools and companies should never use student data for an unauthorized purpose without informed written consent from the student, parent, or guardian.[289] For instance, schools often provide private companies with access to student data with the understanding that the company will work towards enhancing education quality at the school.[290] However, when companies use student data in ways apart from the original purpose to fulfill their own commercial marketing agenda, they have misused student data and violated student privacy rights.[291]

The Bill of Rights would also compel companies to "immediately notify schools, students, and appropriate law enforcement" when a data breach has occurred.[292] In addition, schools would also be responsible for notifying students and parents during a breach and, in general, are encouraged not to collect student data unless sufficient

[285] *See* Strauss, *supra* note 138 (noting the importance of giving students the right to ensure that one's data is accurate).
[286] *See* Strauss, *supra* note 138 (supporting limiting the collection of student data).
[287] *See* Strauss, *supra* note 138 (providing ways that companies can legally access large amounts of student data).
[288] *See* Strauss, *supra* note 138 (presenting an example of a more limited "educational purpose" that would still allow a company to access data, but would curtail their use of that data).
[289] *See* Strauss, *supra* note 138 (stressing the need to obtain consent from students before student data is collected or accessed).
[290] *See* Strauss, *supra* note 138 (validating schools' utilization of outside services in student data management and analysis).
[291] *See* Strauss, *supra* note 138 (explaining companies' misuse of student data for commercial purposes).
[292] *See* Strauss, *supra* note 138 (noting companies' responsibilities when a data breach occurs).

security protections are in place.[293] It is imperative that school administrators understand that proper student data security protocol includes "deleting and de-identifying information after it has been used for its initial primary purposes."[294] Student data collection should be transparent and both school districts and private companies, under the Bill of Rights, would be required to "publish the types of information they collect, the purposes for which the information will be used, and the security practices in place."[295] Most critically, the Bill of Rights would be a revolutionary movement giving students the right to hold schools and private companies responsible for protecting their personal and private information.[296]

In order for the Student Privacy Bill of Rights to have legal backing, several steps must first occur. In order for the Bill of Rights to have associated legal penalties, Congress must pass legislation to apply the Bill of Rights to commercial industries not currently governed by federal data privacy laws.[297] The federal government would then hold meetings with invested parties to develop "codes of conduct" as the mechanism through which the Bill of Rights is implemented on the ground level.[298] The Administration would then work with stakeholders to encourage widespread implementation of the Bill of Rights and the principles would be written into law.[299] Overall, these substantive and well-supported federal efforts demonstrate that student data privacy is a national priority and give hope that major advances in protecting students are on the horizon.

---

[293] *See* Strauss, *supra* note 138 (underscoring students' right to be notified in the event of a breach in data security).
[294] *See* Strauss, *supra* note 138 (describing the additional precautions that companies must take to protect student data).
[295] *See* Strauss, *supra* note 138 (providing methods in which schools and companies can increase transparency between schools and students or parents).
[296] *See* Strauss, *supra* note 138 (recommending that students should be allowed to hold schools and companies accountable for adhering to the Bill's requirements).
[297] *See* Strauss, *supra* note 138 (comparing the Student Privacy Bill of Rights to the Consumer Privacy Bill of Rights).
[298] *See* THE WHITE HOUSE, *supra* note 140 (describing the creation of this type of Bill of Rights).
[299] *See* THE WHITE HOUSE, *supra* note 140 (explaining how such a Bill of Rights could be implemented within the student privacy context).

V. CONCLUSION

This recent period of extraordinary technological growth is redefining and reinventing the model for education in the United States. New technologies are functioning as powerful catalysts for educational reform, but many are also compromising security and privacy for young students. The gravity and immediacy of the student privacy issue is illuminated by the firestorm of national attention, proposed legislative reforms, and private-sector pledges. Elementary and secondary students—one of the nation's most vulnerable populations—need proper safeguards in place to protect their data. In order to amply protect the student privacy, a multi-tiered approach, involving both public and private stakeholders at the local, state, and federal levels, is critical. The efficacy of this approach demands collaboration to establish meaningful protections that fully and comprehensively protect students' and their data. Massachusetts, by empowering students through cutting-edge learning and the promise of data security, is well positioned to be a leader at the intersection of privacy and progress.